UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,772	07/25/2001	Michael L. Wenocur	A-70561/RMA	5626

7590 03/23/2005	**EXAMINER**
FLEHR HOHBACH TEST ALBRITTON & HERBERT LLP	SHERKAT, AREZOO

FLEHR HOHBACH TEST ALBRITTON & HERBERT LLP
Suite 3400
Four Embarcadero Center
San Francisco, CA 94111-4187

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _25 July 2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _19 October 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _1/14/02&2/19/02_.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

Claims 1-20 are presented for examination.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on February 12, 2002 has

been considered by the examiner.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created
doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the
unjustified or improper timewise extension of the "right to exclude" granted by a patent
and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11
F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225
USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA
1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*,
418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be
used to overcome an actual or provisional rejection based on a nonstatutory double
patenting ground provided the conflicting application or patent is shown to be commonly
owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a
terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with
37 CFR 3.73(b).

Claims 1-20 are provisionally rejected under the judicially created doctrine of

obviousness-type double patenting as being unpatentable over claims 1-22 of

copending Application No. 09912901, 901 hereinafter. Although the conflicting claims

are not identical, they are not patentably distinct from each other because of the

following:

Regarding claims 1 and 2, both the instant application and 901 disclose a computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for conducting a secure response session, the program module including instructions for:

A. extracting, by a Client who is establishing a secure response session to the Entity in order to respond to a message from the Entity, the Entity's public key and matching destination address of the Entity from a trusted source or storage means;

B. extracting, by the Client, the Client's public and private key and certificate chain from a trusted source or storage means;

F. verifying, by the Entity, the Client's certificate chain.

The instant application discloses using, the extracted Client's public and private key and certificate chain information along with the previously extracted Entity's destination address to create **a secure unidirectional message to the Entity using the a secure unidirectional message protocol**, a data portion of the Client's message containing a Resource Tag that was included in the message received from the Entity to which this message is a response.

Instead, 901 discloses using, the extracted Client's public and private key and certificate chain information along with the previously extracted Entity's destination address to create **a secure session with the Entity using a secure session protocol**, sending, by the Client, a first Data message after any session setup messages, that contains a Resource Tag that was included in the message received from the Entity to which this client initiated session is a response, and setting up, by the Entity, the session setup portion of the secure session protocol.

The method and system of setting up a secure bi-directional session using a secure bi-directional protocol can be accomplished by creating and sending unidirectional messages from the client to the Entity and/or from Entity to the client. It would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify 901 to expressly include creating a secure unidirectional message to the Entity using the a secure unidirectional message protocol. The motivation for this combination is to provide a secure method to authorize a specific user to access a specific resource such as an email message or a promotional coupon (09912772, Page 4, Par. 0026-0029).

Regarding claim 16, both the instant application and 901 disclose a method for conducting a secure response session from a Client that is establishing a secure response session to an Entity in order to respond to a message from the Entity, said method comprising the steps of:

extracting, by the Client, information including the Entity's public key and

destination address and Client's public and private key and certificate chain from one

or more trusted source (Page 124, claim 16).

The instant application discloses using, by the Client, the extracted information to

create **a secure unidirectional message to the Entity using a secure

unidirectional message protocol**, a data portion of the secure unidirectional

message containing a resource tag that was included in the message received from

the Entity to which the secure unidirectional message is a response.

Instead, 901 discloses using, by the Client, the extracted information to create **a

secure session with the Entity using a secure session protocol**, and sending, by

the Client, a first data message that contains a resource tag that was included in the

message received from the Entity to which this Client initiated session is a response.

The method and system of setting up a secure bi-directional session using a

secure bi-directional protocol can be accomplished by creating and sending

unidirectional messages from the client to the Entity and/or from Entity to the client. It

would have been obvious to a person of ordinary skill in the art at the time of

applicant's invention to modify 901 to expressly include creating a secure unidirectional

message to the Entity using the a secure session protocol and/or a secure

unidirectional message protocol. The motivation for this combination is to provide a

secure method to authorize a specific user to access a specific resource such as an

email message or a promotional coupon (09912772, Page 4, Par. 0026-0029).

Claims 3-15 and 17-20 are rejected by the virtue of depending on rejected base claims.

This is a <u>provisional</u> obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Objections

Claims 1, 2, and 16 are objected to because of the following informalities: There is an extra "the" on page 218, lines 20, 35 and page 220, line 9.

Appropriate correction is required.

Claim 2 is objected to because of the following informalities: claim language states "network transport neutral" when it should clearly be "network transport protocol neutral". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 recites the limitation "the Entity" in the line 13. There is insufficient antecedent basis for this limitation in the claim.

Claim 2 recites the limitation "the Entity" in the line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 recites the limitation "the web page" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim 16 recites the limitation "the Entity" in the line 2. There is insufficient antecedent basis for this limitation in the claim.

Claims 19 and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 19 and 20 recite the limitation "a compact certificate as explained earlier" in the second line. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-5, 7, and 10-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Ross, (U.S. Publication No. 2002/0143885 *filed 19 Nov, 1999* and Ross hereinafter).

Regarding claim 1, Ross discloses a computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for secure unidirectional response message (i.e., JAVA applet)(Page 8, Par. 0116 and Page 9, Par. 0125), the program module including instructions for:

A. extracting, by a Client who is sending a secure response message to the Entity in order to respond to a message from the Entity, the Entity's public key and matching destination address of the Entity from a trusted storage means (Page 11, Par. 0159-0165);

B. extracting, by the Client, the Client's public and private key and certificate

chain from a trusted source or storage means, and C. using, the extracted Client's

public and private key and certificate chain information along with the previously

extracted Entity's destination address to create a secure unidirectional message to the

Entity using the a secure unidirectional message protocol, a data portion of the Client's

message containing a Resource Tag that was included in the message received from

the Entity to which this message is a response (Page 10, Par. 0137-0156); and

D. verifying, by the Entity, the Client's certificate chain (Page 11, Par. 0168-

0171).

Regarding claims 2 and 20, Ross discloses a hardware architecture neutral and

operating system neutral and network transport neutral method for secure unidirectional

response message using less software code and network bandwidth than conventional

systems (i.e., JAVA applet)(Page 8, Par. 0116 and Page 9, Par. 0125), said method

comprising the steps of:

A. extracting, by a Client who is sending a secure response message to the

Entity in order to respond to a message from the Entity, the Entity's public key and

matching destination address of the Entity from a trusted storage means (Page 11, Par.

0159-0165);

B. extracting, by the Client, the Client's public and private key and certificate

chain from a trusted source or storage means, and C. using, the extracted Client's

public and private key and certificate chain information along with the previously

extracted Entity's destination address to create a secure unidirectional message to the

Entity using the a secure unidirectional message protocol, a data portion of the Client's

message containing a Resource Tag that was included in the message received from

the Entity to which this message is a response (Page 10, Par. 0137-0156); and

D. verifying, by the Entity, the Client's certificate chain (Page 11, Par. 0168-

0171).

Regarding claim 3, Ross discloses further comprising: E. performing, by the

Entity, an appropriate application-level action for the received response message (i.e.,

a response module operative to respond by the first user by sending a second email to

the first user, wherein the reader/responder software application program includes an

encryption module operative to encrypt a message of the second email into an

encrypted message using the unencrypted public key of the second user)(Page 3, Par.

0034).

Regarding claim 5, Ross discloses wherein the matching destination address

comprises an e-mail address (Page 10, Par. 0137-0139).

Regarding claim 6, Ross discloses wherein the public key and matching

destination address have been verified previously using a digital signature (verified with

a trusted public key)(Page 10, Par. 0137-0150).

Regarding claim 7, Ross discloses wherein the trusted source or storage means

comprises data from a normal e-mail message (Page 1, Par. 0007).

Regarding claim 10, However, Ross discloses wherein the reader-responder

module can be used to send a key from user 102 to the user 304-308 in order to

enable the user 304-308 to send an e-mail taking advantage of proprietary features of

a first e-mail system (i.e., the email system of user 304-308), to the user 102 who is not

on the first email system (Page 10, Par. 0156-0167).

Regarding claim 11, Ross discloses wherein the Client's keys and certificate

chain are unique to a client, and the Entity authenticates the Client using a unique

certificate and/or using a Resource Tag which was included in the message received

from the Entity to which this session is a response (i.e., email address of the licensed

user)(Page 11, Par. 0168-0171).

Regarding claim 12, Ross discloses wherein the Entity authenticates the Client

using the certificate and/or using a Resource Tag which was included in the message

received from the Entity to which this session is a response (i.e., email address of the

licensed user)(Page 11, Par. 0168-0171).

Regarding claim 13, Ross discloses wherein said verifying by the Entity, further

includes optionally verifying the Resource Tag that is included in the Data portion of the

received message (Page 11, Par. 0168-0171).

Regarding claim 14, Ross discloses wherein the secure unidirectional message

protocol comprises using the Signed-Inside-Enveloped-Data cryptographic primitive

(i.e., encrypted email)(Pages 2-3, Par. 0029).

Regarding claim 15, Ross discloses wherein said entity comprises a merchant

(Page 1, Par. 0007-0010).

Regarding claims 16 and 19, Ross discloses a method for communicating a

secure unidirectional response message from a Client that is sending a secure

response message to the Entity in order to respond to a message from the Entity, said

method comprising the steps of:

extracting, by the Client, information including the Entity's public key and

matching destination address and the Client's public and private key and certificate

chain from one or more trusted source (Page 11, Par. 0159-0165); and

using, by the Client, the extracted information to create a secure unidirectional

message to the Entity using the a secure unidirectional message protocol, a data

portion of the secure unidirectional message containing a resource tag that was

included in the message received from the Entity to which the secure unidirectional

message is a response (Page 10, Par. 0137-0156).

Regarding claim 17, Ross discloses further comprising sending the secure

unidirectional message to the entity (Page 10, Par. 0137-0156).

Regarding claim 18, Ross discloses further comprising verifying, by the Entity,

the Client's certificate chain (Page 11, Par. 0168-0171).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Ross, (U.S. Publication No. 2002/0143885 and Ross hereinafter), in view of Davis

et al., (U.S. Patent No. 6,367,009 and Davis hereinafter).

Teachings of Ross in regards to limitations of claim 2 have been discussed

previously.

Regarding claim 4, Ross does not expressly disclose wherein the Entity's public key comprises an RSA or RSA-based key.

However, Davis discloses wherein the Entity's public key comprises an RSA or RSA-based key (Col. 11, lines 10-67 and Col. 12, lines 1-58).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the method of Ross by including an RSA or RSA-based key as disclosed by Davis. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Davis to enable secure network communications in a non-secure environment (Davis, Col. 1, lines 15-36).

Regarding claims 8-9, Ross does not expressly disclose wherein the trusted source or storage means comprises data received from communicating with a Server via a secure session.

However, Davis discloses wherein the trusted source or storage means comprises data received from communicating with a Server via a secure session (Col. 16, lines 60-67 and Col. 17, lines 1-35).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Ross by including communicating with a Server via a secure session (i.e., SSL/TLS) as disclosed by Davis. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Davis to communicate client's

certificate through secure sessions using Secure Socket Layer protocol or Transaction

Layer Security protocol (Davis, Col. 6, lines 5-55).

Conclusion

The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

Guski et al., (U.S. Patent No. 6,711,679),

Luneau et al., (U.S. Patent No. 5,848,161),

Bunnell, (U.S. Patent No. 6,192,405),

Grimmer, (U.S. Patent No. 5,774,552),

FOX et al., (U.S. Publication No. 2002/0069174),

Shambroom, (U.S. Publication No. 2001/002027),

Zabetian, (U.S. Patent No. 6,327,656),

Azuma, (U.S. Publication No. 2002/0004899), and

Davis et al., (U.S Patent No. 6,367,009).

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-

3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.
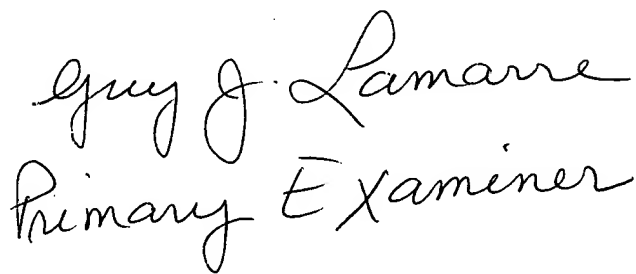
If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Arezoo Sherkat
Patent Examiner
Group 2131
Feb. 23, 2005